UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/974,705	10/10/2001	Marco Macchetti	01AG17653537	7872

27975 7590 11/28/2007

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	

NOTIFICATION DATE	DELIVERY MODE
11/28/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/974,705
Filing Date: October 10, 2001
Appellant(s): MACCHETTI ET AL.

Jack G. Abid
Reg No. 58,237
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on September 7, 2007 and October 11, 2007 appealing from the Office action mailed on May 29, 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is incorrect.

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US2001/0024502	OHKUMA ET AL	9-2001
5,533,127	LUTHER	7-1996

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 21-25, 27-43 and 48-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2001/0024502 to **Ohkuma et al** in view of US Patent 5,533,127 to **Luther**.

As per claim 21, Ohkuma et al substantially teaches a method for converting data between an unencrypted format and an encrypted format, the data being organized in bit words, the method comprising: *converting the data by at least performing a plurality of transformation rounds* (see paragraph 92), *applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array* (page 12, paragraphs 272-274 and figure 30); *applying at least one round key to the state array in at least one of the transformation rounds* (see **Ohkuma et al**, paragraphs 310-311 and 319). **Ohkuma et al** discloses that a matrix obtained by substituting rows and substituting columns and transposing the rows and columns in another matrix (state array) may be used (paragraph 268). As interpreted by examiner the transposing is performed by substituting rows and substituting columns to obtain a transposed MDS matrix (state array) for instance, in figure 31, to obtain y, a transformation is performed to obtain a transposed state of the matrix (paragraph 270 states executing transformation by means of a matrix) therefore, **Ohkuma et al** discloses transposing each of the *rows and columns of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array* (see paragraphs 261-271 see

figure 30). **Ohkuma et al** does not explicitly disclose *exchanging each row with a respective column of the state array to form a transposed state array*. **Luther** in an analogous art discloses an encryption system for two-dimensional binary data using a plurality of rounds or passes. In each pass each row and each column of binary data is encrypted (see column 1, lines 35-39). In one exemplary embodiment, **Luther** suggests that during the process of encryption, when executing steps 211 and 215 in complementing the data signals in the rows and the columns respectively, a substitution of a swap row/column could be implemented to further confuse the data (see column 6, lines 12-16). As interpreted by Examiner, Luther discloses that row 3 and row 4 are being complemented as well as column 4 and column 5 in steps 211 and 215 respectively, and when executing steps 211 and 215 a substitution of a swap row/column would eventually exchange rows 3 and 4 with columns 4 and 5, which meets the recitation of exchanging each of the rows with a respective column. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Ohkuma et al** to perform *exchanging each row with a respective column of the state array to form a transposed state array* to further confuse the data as suggested by **Luther**. One of ordinary skill in the art would have been motivated to do so because it would add another layer of security by hiding the data used in the process of encryption therefore it would be harder for an attacker to be successful in a cryptanalysis attack since the exchanging of row/column is added to confuse the data as suggested by **Luther** (see column 6, lines 12-16).

As per claim 31, Ohkuma et al substantially teaches a device for converting data between an unencrypted format and an encrypted format, the device comprising: at least one

register for storing the data in the form of bit words (see figure 10); and a circuit for *performing a plurality of transformation rounds* (see paragraph 92), *applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array* (page 12, paragraphs 272-274 and figure 30); *applying at least one round key to the state array in at least one of the transformation rounds* (see **Ohkuma et al**, paragraphs 310-311 and 319). **Ohkuma et al** discloses that a matrix obtained by substituting rows and substituting columns and transposing the rows and columns in another matrix (state array) may be used (paragraph 268) . As interpreted by examiner the transposing is performed by substituting rows and substituting columns to obtain a transposed MDS matrix (state array) for instance, in figure 31, to obtain y, a transformation is performed to obtain a transposed state of the matrix (paragraph 270 states executing transformation by means of a matrix) therefore, **Ohkuma et al** discloses transposing each of the *rows and columns of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array* (see paragraphs 261-271 see figure 30). **Ohkuma et al** does not explicitly disclose *exchanging each row with a respective column of the state array to form a transposed state array*. **Luther** in an analogous art discloses an encryption system for two-dimensional binary data using a plurality of rounds or passes. In each pass each row and each column of binary data is encrypted (see column 1, lines 35-39). In one exemplary embodiment, **Luther** suggests that during the process of encryption, when executing steps 211 and 215 in complementing the data signals in the rows and the columns respectively, a substitution of a swap row/column could be implemented to further confuse the data (see column 6, lines 12-16). As interpreted by Examiner, Luther discloses that row 3 and row 4 are being complemented as well as column 4

and column 5 in steps 211 and 215 respectively, and when executing steps 211 and 215 a substitution of a swap row/column would eventually exchange rows 3 and 4 with columns 4 and 5, which meets the recitation of exchanging each of the rows with a respective column. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Ohkuma et al** to perform *exchanging each row with a respective column of the state array to form a transposed state array* to further confuse the data as suggested by **Luther**. One of ordinary skill in the art would have been motivated to do so because it would add another layer of security by hiding the data used in the process of encryption therefore it would be harder for an attacker to be successful in a cryptanalysis attack since the exchanging of row/column is added to confuse the data as suggested by **Luther** (see column 6, lines 12-16).

As per claims 22 and **32**, the references as combined above disclose the limitation of *wherein said at least one register stores bit words as 8-bit words* (**Ohkuma et al**, page 6, paragraph 128).

As per claims 23 and **33**, the references as combined above disclose the limitation of *wherein said circuit operates on a state array comprising a 4x4 matrix of bit words* (**Ohkuma et al**, page 6, paragraph 128).

As per claims 24 and **34**, the references as combined above disclose *said circuit in performing a plurality of transformation rounds performs at least 10 transformation rounds* (**Ohkuma et al**, page 4, paragraph 92).

As per claim 25, the references as combined above disclose *performing at least one* stage or *round on a non-transposed matrix* (state array); (see **Ohkuma et al**, paragraph 241) stating "the final round does not include any higher-level MDS". Performing at least one round on a non-transposed state array is well known as disclosed in Rijndael cipher algorithm. (See also **Ohkuma et al**, page 4, paragraph 87, and prior art figure 4 of Applicant's disclosure).

As per claim 27, the references as combined above disclose the limitation of *wherein the at least one round key is transposed* (see **Ohkuma et al**, figure 3 and figure 6 and page 5, paragraph 109).

As per claim 28 the references as combined above disclose the limitation of *adding code to transpose the at least one round key* (see **Ohkuma et al**, page 6, paragraphs 140-142; see also page 7, paragraph 147).

As per claim 29, the references as combined above disclose the limitation of *wherein the at least one round key comprises a plurality of round keys, each corresponding to a respective transformation round and being applied according to a round key schedule* (see **Ohkuma et al**, page 7, paragraph 147).

As per claim 30, the references as combined above disclose the limitation of wherein the *round key schedule comprises a transposed round key schedule* (see **Ohkuma et al**, page 7, paragraph 147). The transformation applied to the round key schedule by diffusing random keys and applied different constants at different units of rounds meets the recitation of a transposed round key schedule.

As per claim 35, the references as combined above disclose *wherein said circuit comprises at least one S-box processing module, said at least one S-box processing module operating on a group of bit words defining a cell of a column of the state array* (see **Ohkuma et al**, figure 6, 112).

As per claim 36, the references as combined above disclose *wherein the at least one S-box processing module comprises a plurality of S-box modules, each of the plurality of S-box modules operating on a corresponding cell of a column of the state array* (see **Ohkuma et al**, figure 6, 112).

As per claim 37, the references as combined above disclose the limitation of *wherein the column of the state array comprises four cells* (**Ohkuma et al**, page 4, paragraph 92).

As per claims 38-39, the references as combined above disclose that the invention can be performed by any number of modules and any combination of bits wherein the circuit further

comprises a plurality of shift column modules, (**Ohkuma et al**, page 3, paragraphs 62-65); and further discloses shift up can be performed (**Ohkuma et al**, page 5, paragraph 117); column mix is also a well known process as disclosed in Rijndael cipher algorithm (**Ohkuma et al**, page 1, paragraph 5 and page 4, paragraph 87) that meets the recitation of *each of said plurality of shift column modules to perform a column shift operation on a column of the state array* and the limitation of *wherein a column shift operation performed by each of said plurality of shift column modules generates shift column data, and wherein said circuit further comprises a single mix column module to perform column mix operations on shift column data.*

As per claims 40-43, the references as combined above disclose an encryption and decryption apparatus that meets the recitation of *encoder* for converting data from an unencrypted data format to an encrypted data format and a *decoder* for converting data from an encrypted data format to an unencrypted data format (**Ohkuma et al**, page 15, paragraph 343-349). **Ohkuma et al** further discloses an encryption and decryption apparatus formed as a semiconductor device that meets the recitation of *embedded system for use in a smart card* (**Ohkuma et al**, page 15, paragraph 343-349).

As per claim 48, **Ohkuma et al** substantially teaches a method for converting data between an unencrypted format and an encrypted format, the data being organized in bit words, the method comprising: *converting the data by at least performing a plurality of transformation rounds for converting the data* (see paragraph 92) comprising, *applying at least one transformation to a two-dimensional array of rows and columns of 8-bit words defining a state*

array (page 12, paragraphs 272-274 and figure 30) comprising a *4x4 matrix of bit words* (**Ohkuma et al**, page 6, paragraph 128); *applying at least one round key to the state array in at least one of the transformation rounds* (see **Ohkuma et al**, paragraphs 310-311 and 319). **Ohkuma et al** discloses that a matrix obtained by substituting rows and substituting columns and transposing the rows and columns in another matrix (state array) may be used (paragraph 268). As interpreted by examiner the transposing is performed by substituting rows and substituting columns to obtain a transposed MDS matrix (state array) for instance, in figure 31, to obtain y, a transformation is performed to obtain a transposed state of the matrix (paragraph 270 states executing transformation by means of a matrix) therefore, **Ohkuma et al** discloses transposing each of the *rows and columns of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array* (see paragraphs 261-271 see figure 30). **Ohkuma et al** does not explicitly disclose *exchanging each row with a respective column of the state array to form a transposed state array*. **Luther** in an analogous art discloses an encryption system for two-dimensional binary data using a plurality of rounds or passes. In each pass each row and each column of binary data is encrypted (see column 1, lines 35-39). In one exemplary embodiment, **Luther** suggests that during the process of encryption, when executing steps 211 and 215 in complementing the data signals in the rows and the columns respectively, a substitution of a swap row/column could be implemented to further confuse the data (see column 6, lines 12-16). As interpreted by Examiner, Luther discloses that row 3 and row 4 are being complemented as well as column 4 and column 5 in steps 211 and 215 respectively, and when executing steps 211 and 215 a substitution of a swap row/column would eventually exchange rows 3 and 4 with columns 4 and

5, which meets the recitation of exchanging each of the rows with a respective column. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Ohkuma et al** to perform *exchanging each row with a respective column of the state array to form a transposed state array* to further confuse the data as suggested by **Luther**. One of ordinary skill in the art would have been motivated to do so because it would add another layer of security by hiding the data used in the process of encryption therefore it would be harder for an attacker to be successful in a cryptanalysis attack since the exchanging of row/column is added to confuse the data as suggested by **Luther** (see column 6, lines 12-16).

As per claim 49, the references as combined above disclose the limitation of *wherein the at least one round key is transposed before being applied to the state array* (see **Ohkuma et al**, figure 3 and figure 6 and page 5, paragraph 109).

As per claim 50 the references as combined above disclose the limitation of *adding code to transpose the at least one round key* (see **Ohkuma et al**, page 6, paragraphs 140-142; see also page 7, paragraph 147).

As per claim 51, the references as combined above disclose the limitation of *wherein the at least one round key comprises a plurality of round keys, each corresponding to a respective transformation round and being applied according to a round key schedule* (see **Ohkuma et al**, page 7, paragraph 147).

(10) Response to Argument

Appellant's arguments with respect to **claims 21, 31, and 48** are not persuasive. Appellant argues (see pages 9-10 of Appeal Brief) "*The Examiner specifically contends that rows 3 and 4 are complemented and columns 4 and 5 are complemented, thereby disclosing the claimed transposition feature. Notwithstanding that complementing does not equal transposing, the Examiner contends that rows 3 and 4 are complemented in Figure 6, and that columns 4 and 5 are complemented in Figure 7. Appellants note that this arrangement of Luther does not disclose the claimed transposition... Therefore, Appellants submit that Luther fails to disclose the claimed feature of exchanging each of the rows with a respective column of the state array to form a transposed state array.*" Examiner respectfully disagrees with Appellant's misinterpretation because it is the "swap substitution" of row and column not the "complementing" that Examiner interprets as meeting the claimed limitation exchanging each row with a respective column to form a transposed state array. In fact, Luther discloses in column 6, lines 12-18:

"When executing steps S211 and S215 for complementing the data signals in the rows and the columns respectively, a substitution of a swap row/column or a shift row/column end around function could be implemented to further confuse the data."

Therefore, Luther teaches complementing each of the rows with a respective column for a state array and Luther clearly suggests implementing a substitution of a swap (i.e. transposing) of rows with respective columns to further confuse the data.

Regarding the dependent claims, it is believed that the rejections should be sustained for the same reasons discussed above with respect to claims 21, 31, and 48 as no further arguments were presented by Appellant.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Carl Colin/
Carl Colin
Patent Examiner, A.U. 2136
November 15, 2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

/Christopher Revak/
Christopher Revak
Primary Examiner, GAU 2131

Gilberto Barron Jr.
SPE 2132

STMICROELECTRONICS S.R.L.
VIA C. OLIVETTI, 2
20041 AGRATE BRIANZA, ITALY